EC-Council Certified Security Analyst (ECSA)

Course Summary

Description

You are an ethical hacker. In fact, you are a Certified Ethical Hacker. Your last name is Pwned. You dream about enumeration and you can scan networks in your sleep. You have sufficient knowledge and an arsenal of hacking tools and you are also proficient in writing custom hacking code.

Is that enough?

Can you become an industry accepted security professional? Will organizations hire you to help them protect their systems? Do you have any knowledge in applying a suitable methodology to conduct a penetration test for an enterprise client?

The ECSA penetration testing certification is a security credential like no other!

The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and elevates your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing published penetration testing methodology

- Focuses on pentesting methodology with an emphasis on hands-on learning
- The exam will now have a prerequisite of submitting a pentesting report
- The goal of these changes is to make passing ECSA more difficult; therefore making it a more respected certification

From the commencement of the 5 day class and the activation of the ECSA Dashboard on ASPEN, you will have 60 days in total to submit your penetration testing report based on the challenge scenario, which will prove that you understand the concepts thought in the course. This is the eligibility criterion to enable you to challenge the ECSA exam. The Final ECSA Exam is a Multiple Choice Question Exam. The ECSA v9 exam includes 2 required stages.

Report writing stage requires candidates to perform various penetration testing exercises on iLabs before submitting a penetration test report for assessment. Candidates that submit reports to the required standards will be provided with exam vouchers for the multiple choice exam.

Multiple choice exams are proctored online through the Exam portal. ECSA v9 Exam info:

- Credit Towards Certification: ECSA v9
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 Hours

EC-Council Certified Security Analyst (ECSA)

Course Summary (cont'd)

Topics

- Security Analysis and Penetration Testing Methodologies
- TCP IP Packet Analysis
- Pre-penetration Testing Steps
- Information Gathering Methodology
- Vulnerability Analysis
- External Network Penetration Testing Methodology
- Internal Network Penetration Testing Methodology
- Firewall Penetration Testing Methodology
- IDS Penetration Testing Methodology
- Web Application Penetration Testing Methodology
- SQL Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Network Penetration Testing Methodology
- Mobile Devices Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Test Actions
- Password Cracking Penetration Testing
- Router and Switches Penetration Testing
- Denial-of-Service Penetration Testing
- Stolen Laptop, PDAs and Cell Phones Penetration Testing
- Source Code Penetration Testing
- Physical Security Penetration Testing
- Surveillance Camera Penetration Testing
- VoIP Penetration Testing
- VPN Penetration Testing
- Virtual Machine Penetration Testing
- War Dialing
- Virus and Trojan Detection
- Log Management Penetration Testing
- File Integrity Checking
- Telecommunication and Broadband Communication Penetration Testing
- Email Security Penetration Testing
- Security Patches Penetration Testing
- Data Leakage Penetration Testing
- SAP Penetration Testing
- Standards and Compliance
- Information System Security Principles
- Information System Incident Handling and Response
- Information System Auditing and Certification

Audience

This course is designed for:

- Ethical Hackers
- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals

Prerequisites

There are no prerequisites for this course.

Duration

Five days